

Appl. No: 09/635,823  
Amdt. Dated July 6, 2004  
Reply to Office Action of April 5, 2004

### REMARKS/ARGUMENTS

Prior to this Amendment, claims 1-4, 6-11, 13, 14, and 16-23 were pending in this application. Claims 11 and 16 are canceled. Claim 1 is amended to clarify that the monitoring tool uploads data to a central site by first splitting the collected data into smaller files or data chunks and second transferring each of the smaller files over a network link based on a network protocol, which may involve the smaller files being packetized. New claim 24 is added to protect the feature of scheduling the transferring the collected data to the central site based on storage activity or availability at the central site. No new matter is added with support found at page 12, lines 15-28 of Applicants' specification.

Claims 1-4, 6-10, 13, 14, and 17-24 remain in the application for consideration by the Examiner.

#### Rejections under 35 U.S.C. 112

In the Office Action, claim 16 was rejected under 35 U.S.C. 112. Claim 16 is canceled by this Amendment.

#### Rejections under 35 U.S.C. 102

In the Office Action, claims 1 and 2 were rejected under 35 U.S.C. 102 as being anticipated by U.S. Pat. No. 5,758,071. This rejection is respectfully traversed.

Claim 1 calls for a monitoring tool that uploads data collected by a set of data collectors to a central site. The uploading comprises "splitting the data into multiple data chunks and transmitting the data chunks separately to the central site." The transmitting comprises transferring each of the data chunks over a link of the network according to "according to a transfer protocol wherein each of the data chunks may be subject to packetization." Hence, as amended, claim 1 requires that not only is the transferred data subjected to standard packetization according to a network transfer protocol but also the monitoring tool acts to first subdivide the gathered data into data chunks. The Office Action argues that packetization is standard for transfer of digital data over communication links,

Appl. No: 09/635,823  
Amdt. Dated July 6, 2004  
Reply to Office Action of April 5, 2004

and Applicants agree that standard packetization is not novel. However, Burgess fails to show a monitoring tool that processes gathered data into smaller files prior to sending the files (via standard protocols). For this reason, the rejection of claim 1 under Burgess is improper and should be withdrawn.

Further, at the central site, the data chunks are merged into a data file that is then loaded into a database. The use of smaller chunks or smaller files rather than one large stream of data enables the central site to more effectively receive the data without congesting the receiving web server and more likely losing data. This is more important when the central site may be receiving collected data from numerous monitoring tools. As stated in the last Amendment, this technique is different than typical packetization used in digital transfer protocols, and to make this difference clearer, the use of the phrase "data chunks" was chosen rather than packets. The use of subsets of data or chunks also enables the monitoring tools to perform more effectively. In this regard, Claim 23 protects the idea that the configuration file processed by the monitoring tool (see dependent claim 6) may be used to define the size of the data chunk used by the monitoring tool. Burgess provides no teaching of sending the collected data from the agent 16 to the listener 18 in smaller chunks. Hence, claim 1 is not shown or suggested by Burgess, and claim 2 is allowable as depending from an allowable base claim.

New claim 24, which depends from claim 1, is added to further protect the concept of controlling the data receipt and processing load placed on the central site's facilities. Claim 24 calls for the monitoring tool to listen to a storage location at the central site for an available data file and when the data file is available to invoke the uploading process. Burgess does not teach scheduling of transmittal of gathered data in this manner. Hence, claim 24 is allowable for this additional reason.

Appl. No: 09/635,823  
Amdt. Dated July 6, 2004  
Reply to Office Action of April 5, 2004

**Rejections under 35 U.S.C. 103**

Additionally, the Office Action rejected claims 3-4, 6-11, 13, 14, 18, and 23 under 35 U.S.C. 103 as being unpatentable over Burgess in view of U.S. Pat. No. 6,681,243 ("Putzolu"). This rejection is respectfully traversed.

Claims 3-4 and 6-8 depend from claim 1 and are believed allowable as depending from an allowable base claim. Additionally, claim 6 calls for accessing a configuration file to determine which data collectors to run on which target devices. The monitoring tool then launches these data collectors on the target devices. As noted in the Office Action in the first full paragraph of page 6, Burgess fails to teach a monitoring tool configured to perform this function.

The Office Action then argues that one skilled in the art would have been motivated to look for teachings in the art for this function and would have modified Burgess with the teaching of Putzolu at col. 12, line 49 through col. 13, line 3 and col. 12, lines 27-37. However, Putzolu fails to teach a monitoring tool accessing a configuration file to determine which data collectors to run on which target devices. Putzolu teaches the use of a plurality of mobile agents to monitor network devices. Each network device is configured with a "proactive environment" to execute the agent. The agents each have an "access control list" that defines which devices the agent MAY work on and which services on that device the agent may use or access (see, col. 12, line 3-7 and col. 12, lines 47-67).

During operation, Putzolu teaches at col. 12, line 3-7 that the receiving proactive environment determines from the agent's access control list if that agent has permission to work on that device. Putzolu does NOT teach a monitoring tool on a different network device that accesses a configuration file to determine which data collectors to launch on which machines. A management console application 9 on a management node 30 (see, Figure 1 of Putzolu) may pick and choose which agents are run on which devices but there is no teaching that this application 9 accesses a configuration file to make such a determination (nor even that the application checks each of the numerous access control lists

Appl. No: 09/635,823  
Amdt. Dated July 6, 2004  
Reply to Office Action of April 5, 2004

to load agents where they are permitted). Hence, the combination of Burgess and Putzolu would not produce the method of claim 6, and the rejection based on this combination of references is improper.

Independent claim 9 is directed to a system for monitoring the configuration and/or status of devices on a network. The arguments provided for allowing claim 6 are equally applicable to claim 9 because claim 9 calls for a monitoring application running on a first device of a network. The monitoring application acts to access "a configuration file to determine which of the data collector modules to run on which ones of the target devices." Neither Burgess nor Putzolu teach such a monitoring application. Specifically, the agents 110, 120 in Figure 1 of Putzolu include agent-specific access control lists that define which nodes or devices on the network 4 they can run but there is no teaching of a configuration file on the node 30 that can be accessed by the management console application or another application to determine which agents 110, 120 to launch on which nodes or devices on the network 4. Hence, the method of claim 9 is not shown or suggested by the combined teaching of these references. Claim 10, 13, and 14 depend from claim 9 and are believed allowable as depending on an allowable base claim.

Independent claim 18 is directed to a method for monitoring a set of information for a plurality of computer devices. As explained in the prior Amendment, the method comprises starting a data collection tool on one of the network devices, e.g., the master machine 20 shown in Figure 2. A configuration file is then retrieved by the data collection tool and then used to "identify a set of the network devices to be monitored." Then, one or more data collectors is run on only the identified network devices, with each of the collectors collecting differing sets of information. The collected data is then sent to the device running the data collection tool.

The Office Action acknowledges that Burgess fails to teach "using the configuration file to identify a set of the network devices to be monitored" and cites Putzolu for teaching this feature of the method of claim 18. However, as

Appl. No: 09/635,823  
Amdt. Dated July 8, 2004  
Reply to Office Action of April 5, 2004

discussed with respect to claims 6 and 9, Putzolu fails to teach using a configuration file that is used to define how monitoring is to be performed. More particularly, with respect to claim 18, Putzolu does not teach in the citations on column 12 and 13 that a configuration file is used to determine which network devices are to be monitored and then running one or more data collectors on the identified network devices. Instead, Putzolu teaches that each agent has an access control list that the "receiving proactive environment" running on a target device uses to determine whether or not to allow the agent to run on that particular target device.

The use of a configuration file to identify which devices to monitor is not suggested by the access control list, which is individual to each agent. Further, Putzolu teaches other techniques for defining which devices to monitor such as at col. 11, lines 49-53 where an agent may decide on its own to move to another network device (and at this point, the receiving device would check the agent's access control list for permission) or the management console application may send it a message (such as application 9 in Figure 1, which is not shown to use a configuration file to determine which agents should be moved to which network devices). For at least these reasons, it is believed that Putzolu does not overcome the admitted deficiencies in Burgess and the Office should allow claim 18.

Claim 23 depends from claim 1 and is believed allowable as depending from an allowable base claim. Further, no explanation for the 103 rejection of claim 23 is provided in the Office Action. Applicants' request that specific citations be provided to the references so that they can properly respond or that the rejection be withdrawn.

Additionally, in the Office Action, claims 3, 4, 7 and 8 were rejected as being unpatentable over Burgess in view of U.S. Pat. No. 5,732,275 ("Kullick"). This rejection is traversed.

Appl. No: 09/635,823  
Amdt. Dated July 6, 2004  
Reply to Office Action of April 5, 2004

Claims 3, 4, 7, and 8 depend from claim 1, which is believed to be in condition for allowance. Hence, claims 3, 4, 7, and 8 are believed allowable over Burgess taken alone. Further, Kullick fails to overcome the deficiencies in Burgess. As indicated in the last Amendment, Kullick does not teach transferring collected data in data chunks or subsets and then merging them at a central site.

In the Office Action, claim 17 was rejected under 103(a) as being unpatentable over Burgess in view of Putzolu and further in view of Kullick. Claim 17 depends from claim 9 and is believed allowable for the reasons for allowing claim 9. Further, Kullick fails to overcome the deficiencies pointed out in the combined teachings of Burgess and Putzolu with reference to claim 9.

Yet further, in the Office Action, claims 18-22 were rejected under 103(a) as being unpatentable over U.S. Pat. No. 6,182,157 ("Schlener") in view of Putzolu further in view of U.S. Pat. No. 5,828,830 ("Ranagaraian"). This rejection is traversed based on the following remarks.

Independent claim 18 is directed to a method for monitoring a set of information for a plurality of computer devices. As explained in the prior Amendment, the method comprises starting a data collection tool on one of the network devices, e.g., the master machine 20 shown in Figure 2. A configuration file is then retrieved by the data collection tool and then used to "identify a set of the network devices to be monitored." Then, one or more data collectors is run on only the identified network devices, with each of the collectors collecting differing sets of information. The collected data is then sent to the device running the data collection tool.

The Office Action acknowledges that Schlener fails to teach "using the configuration file to identify a set of the network devices to be monitored" and cites Putzolu for teaching this feature of the method of claim 18. However, as discussed with respect to claims 6 and 9, Putzolu fails to teach using a configuration file that is used to define how monitoring is to be performed. More particularly, with respect to claim 18, Putzolu does not teach in the citations on

Appl. No: 09/635,823  
Amdt. Dated July 6, 2004  
Reply to Office Action of April 5, 2004

column 12 and 13 that a configuration file is used to determine which network devices are to be monitored and then running one or more data collectors on the identified network devices. Instead, Putzolu teaches that each agent has an access control list that the "receiving proactive environment" running on a target device uses to determine whether or not to allow the agent to run on that particular target device.

The use of a configuration file to identify which devices to monitor is not suggested by the access control list, which is individual to each agent. Further, Putzolu teaches other techniques for defining which devices to monitor such as at col. 11, lines 49-53 where an agent may decide on its own to move to another network device (and at this point, the receiving device would check the agent's access control list for permission) or the management console application may send it a message (such as application 9 in Figure 1, which is not shown to use a configuration file to determine which agents should be moved to which network devices). Rangaraian also fails to teach the using of a configuration file to identify which network devices to monitor as called for in claim 18. For at least these reasons, it is believed that Putzolu does not overcome the admitted deficiencies in and the Office should allow claim 18.

Claims 19-22 depend from claim 18 and are believed allowable as depending from an allowable base claim. Claim 19 calls for the configuration file to comprise a listing of data collectors to be run on each of the identified network devices. As discussed with reference to claims 6 and 9, this is not taught by Putzolu, and it is also not taught by Rangaralan or Schlener. Claim 19 is allowable over the references for this additional reason.

In claim 20, the configuration file further lists sets of information for the collectors to pass to the tool. Hence, the data collection tool uses the configuration file not only to select which network devices to monitor but also which collectors to run on each of such selected devices and which portions of the collected data to gather. This feature is not shown by the combined teaching of the references, and the rejection of claim 20 should be withdrawn.

Appl. No: 09/635,823  
Amdt. Dated July 6, 2004  
Reply to Office Action of April 5, 2004

**Conclusions**

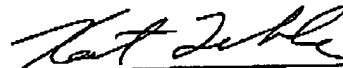
The additional references made of record in the Office Action but not relied upon have been considered but are believed no more relevant than those cited and relied upon. The pending claims are believed allowable over these additional references considered alone or in any combination.

In view of all of the above, the claims are now believed to be allowable and the case in condition for allowance which action is respectfully requested. Should the Examiner be of the opinion that a telephone conference would expedite the prosecution of this case, the Examiner is requested to contact Applicants' attorney at the telephone number listed below.

No fee is believed due with this Amendment, but any fee deficiency associated with this submittal may be charged to Deposit Account No. 50-1123.

Respectfully submitted,

July 6, 2004



Kent A. Lembke, Reg. No. 44,866  
Hogan & Hartson LLP  
One Tabor Center  
1200 17th Street, Suite 1500  
Denver, Colorado 80202  
(720) 406-5378 Tel  
(720) 406-5301 Fax